

Appl. No.: 10/052,094
Amdt. Dated: July 22, 2004
Reply to Final Rejection of April 23, 2004

APP 1365

REMARKS/ARGUMENTS

The Examiner rejected claims 1-4, 6-10, and 12-15 as unpatentable, 35 USC 103(a), over Murakawa patent application US 2001/0020273 A1, December 1, 2000 (hereinafter Murakawa) in view of Calhoun, patent 6,463,475 B1, October 8, 2002 (hereinafter Calhoun). The Examiner further rejected claims 5, 11, and 15 as unpatentable, 35 USC 103(a), over Murakawa in view of Calhoun, in further view of Poier et al. patent application US 2002/0124090 A1, August 20, 2001 (hereinafter Poier). In response thereto, applicants have amended claims 1, 8, and 12 to include limitations of claim 4 and as such, claims 1, 8, and 12 do not raise the issue of new matter. Accordingly, applicants have cancelled claim 4 and amended claims 6 and 10 in accordance with the changes made to claims 1 and 8. In addition, to expedite prosecution of this application, applicants have cancelled claims 2-5, 7, 9, 11, and 13-15.

Applicants' invention is directed at allowing devices on an external network to access a device on a local network wherein the device on the local network is protected by an apparatus, such as a network address translator (NAT), that controls access to the local network. Typically, such a blocking apparatus must be reconfigured to allow external devices to access the local device. However, reconfiguring blocking apparatus to allow external access is not preferred because it is difficult to do and because it becomes unmanageable and creates security risks for the local network as the number of external devices seeking access increases. Applicants' invention allows external devices to access the local device without performing these reconfigurations. (Specification, page 1, line 12 to page 2, line 3).

More specifically, each of amended independent claims 1, 8, and 12 recites a method or system by which any of a plurality of second devices can bypass an access blocking apparatus (such as a NAT) and communicate with a first device when the first device is on a local network, the second devices are external to this local network, and the access blocking apparatus separates the first and second devices. Significantly, each claim recites a hub that terminates a virtual pipe from the first device and then assigns this first device an IP address. This IP address gives the local device an appearance on the external network. Any of the second devices can then communicate with the first device by addressing the communications to this IP address. These communications are routed to the hub, which then routes the communications through the pipe to the first device, thereby bypassing the access blocking apparatus without having to perform reconfigurations. Significantly, any number of external devices can communicate with the local device based on establishing this single virtual pipe.

Appl. No.: 10/052,094
Amdt. Dated: July 22, 2004
Reply to Final Rejection of April 23, 2004

APP 1365

Murakawa also teaches a method whereby devices on an external network can access a device on a local network that is protected by a NAT. However, Murakawa's teachings are divergent from applicants' invention as recited by claims 1, 8, and 12 and significantly, fail to resolve the problems applicants' invention overcomes. Specifically, Murakawa teaches that a security gateway, which includes NAT functionality, separates the local network from the external network. Each external device needing to access the local device establishes its own virtual pipe to this gateway. The gateway then assigns a separate IP address to each external device, which addresses give the external devices appearances on the local network. (Murakawa, paragraphs 91-98).

Accordingly, Murakawa's teachings are the opposite of applicants' invention. Under Murakawa, the external devices establish virtual pipes and are assigned the IP addresses, which give the external devices appearances on the local network. In accordance with applicants' invention, the local device establishes the virtual pipe and is assigned the IP address, which gives the local device an appearance on the external network. As important, Murakawa's teachings also fail to obviate applicants' invention because under Murakawa, the NAT must be properly reconfigured to give the external devices access to the local network (see Murakawa, paragraph 98: "gateway 203 distributes to outside PC 101, *through the NAT technology*, a private IP address"). As described above, applicants' invention is directed at preventing such reconfigurations. (Specification, page 1, line 32 to page 2, line 3). More importantly, for each external device needing access to the local device, a separate virtual pipe must be established under Murakawa. As discussed above, applicants' invention only requires a single virtual pipe to give any number of external devices access to the local device. Again, this is significant because every additional virtual pipe established under Murakawa requires an additional NAT reconfiguration and further opens the local network to security risks, the exact problems applicants' invention overcomes.

Under Calhoun, devices on an external network access a local network by establishing tunnel connections through the external network to the local network. However, contrary to applicants' invention as recited by claims 1, 8, and 12, Calhoun is not directed at bypassing blocking apparatus in the local network. Rather, Calhoun is concerned with controlling these incoming tunnel connections to the local network in order to manage the security and resources of the local network. Calhoun performs this management through a "tunnel switch" inserted in the local network. For each incoming tunnel from the external network, this "tunnel switch" terminates the incoming tunnel and initiates a corresponding "switched tunnel" to the local network resources. It then routes traffic from the incoming tunnels to the desired resource through each tunnels corresponding "switched tunnel".

Appl. No.: 10/052,094
Amdt. Dated: July 22, 2004
Reply to Final Rejection of April 23, 2004

APP 1365

(Calhoun, column 1, line 24 to column 2, line 18; column 3, line 58 to column 4, line 44). Accordingly, like Murakawa, Calhoun teaches the external devices establishing the tunnels to the local network rather than the local device establishing a tunnel to the external network, as claims 1, 8, and 12 recite. In addition, Calhoun fails to teach or suggest the assigning of an IP address to a device to give it an appearance on another network.

As important, each external device needing access to the local network needs a separate tunnel to the "tunnel switch" and a separate "switched tunnel" to the network resources. Again, in accordance with applicants' invention, multiple external devices can access the same local device using a single virtual pipe. It should be further noted that Calhoun discusses a "bundling" concept, in which multiple tunnels from a single external user to the "tunnel switch" are bundled by the "tunnel switch" to the same "switched tunnel". (Calhoun, column 8, line 63 to column 9, line 18). Again, this is different from applicants' invention because the "tunnel switch" is still terminating multiple tunnels from the external user and because Calhoun fails to teach or suggest bundling multiple external users/devices over a single tunnel. Accordingly, Murakawa and Calhoun, alone or in combination, fail to teach or suggest independent claims 1, 8, and 12.

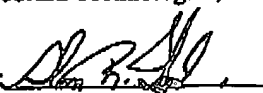
Claims 6 and 10 depend from claims 1 and 8 and are therefore novel and nonobvious for the same reasons as set forth above.

Since Murakawa, Calhoun, and Poier alone or in combination do not teach or suggest applicants' novel methods and apparatus as set forth in applicants' amended claims, applicants respectfully request withdrawal of the Final Rejection, entry of this amendment, and favorable reconsideration and allowance of claims 1, 6, 8, 10, and 12.

Applicants believe that this application is now in condition to be passed to issue, and such action is also respectfully requested. However, if the Examiner deems it would in any way expedite the prosecution of this application, he is invited to telephone applicants' agent at the number given below.

Respectfully submitted,

Telcordia Technologies, Inc.

By: 
Glen Farbanish
Reg. No. 50561
Tel.: (732) 699-3668